

Quel impact sur les infrastructures IP ?

Comment la convergence de la voix et des réseaux de données a-t-elle influencé l'évolution des infrastructures de communication ?


Comment restituer la qualité des communications voix dans une infrastructure IP

Comment garantir une disponibilité du service de téléphonie sur IP du même niveau que les solutions traditionnelles ?

Comment s'assurer de la sécurité du service de téléphonie sur IP ?



Architect of an Open World™



Les dirigeants d'entreprises exigent que leur système d'information soit plus réactif, plus communicant, plus sûr, plus accessible aux collaborateurs mobiles, plus flexible et moins coûteux.

Afin de répondre à ces exigences, les infrastructures de communication ont subi de profondes mutations au cours de ces dernières années.

Parmi les principaux facteurs à l'origine de ces changements, l'avènement de la convergence de la téléphonie et des réseaux informatiques a probablement été le plus structurant, suivi d'une forte percée des technologies mobiles dans l'entreprise.

Comment la convergence de la téléphonie et de l'informatique a-t-elle contribué à l'évolution des infrastructures de communication ?

Comment les défis liés à la qualité de service et à la sécurité sont-ils abordés et traités ?

Quelle est la situation aujourd'hui ?

Ce Livre Blanc vous propose de dresser un panorama des principales évolutions des infrastructures de communication de l'entreprise.

Sommaire

La révolution dans la téléphonie

Comment la convergence de la voix et des réseaux de données a-t-elle influencé l'évolution des infrastructures de communication ?

Les premiers pas.....	5
Une histoire de technologie et de coût.....	6
Une histoire d'adaptation de l'organisation.....	6
Une histoire de révolution dans l'usage de la téléphonie.....	6
Une histoire d'infrastructure.....	6

La maîtrise de la qualité vocale

Comment restituer la qualité des communications voix dans une infrastructure IP ?

Un défi difficile à relever	7
De l'approche « Integrated Services » à l'approche « Differentiated Services »	7
La classification des flux a permis de déployer l'approche « Differentiated Services »	7

Le challenge de la disponibilité

Comment garantir une disponibilité du service de téléphonique sur IP du même niveau que les solutions traditionnelles ?

Le challenge de la disponibilité d'une infrastructure IP.....	9
L'émergence d'infrastructures physiques maillées.....	9
L'adaptation de l'architecture logique au maillage de l'infrastructure physique.....	10
Pallier les limites du protocole STP	11

La confidentialité des échanges

Comment s'assurer de la sécurité du service de téléphonie sur IP ?

La confidentialité des échanges est un point clef de la ToIP	12
La ToIP plonge la Téléphonie au cœur des menaces sur l'infrastructure IP	12
Le contrôle d'accès de l'utilisateur	13
Le contrôle de conformité du poste de travail.....	14

La révolution dans la téléphonie

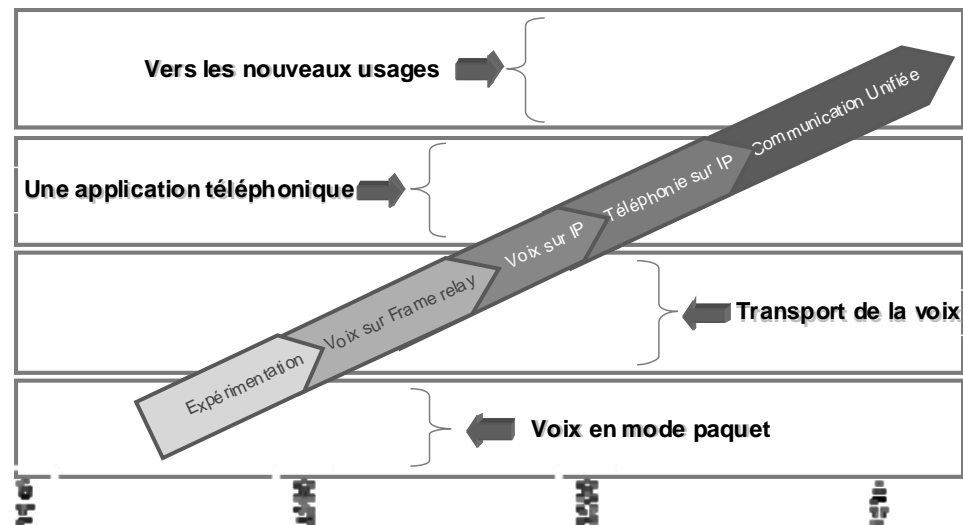
Comment la convergence de la voix et des réseaux de données a-t-elle influencé l'évolution des infrastructures de communication ?

Les premiers pas

En préalable à la mise en œuvre de la convergence de la voix et des réseaux, il a été indispensable de réaliser techniquement le transport des flux voix et données, en un mode paquet, sur une infrastructure de communication commune. Le transport sous forme de paquets, d'un flux voix, que certains constructeurs informatiques avaient déjà tenté de réaliser au milieu des années 1980, est devenu réalité au milieu des années 1990 grâce au protocole Frame Relay qui permettait de s'affranchir des nombreux acquittements protocolaires des autres protocoles.

Le transport proprement dit de la voix dans des paquets d'informations était effectivement résolu mais ne répondait que partiellement à l'objectif de convergence des infrastructures voix et données. En effet, la technologie Frame Relay ne couvrait que la portion des intersites des infrastructures (WAN). Assez rapidement, dès la fin des années 1990, il est devenu envisageable, grâce au protocole IP, d'acheminer les communications téléphoniques de bout en bout au travers d'une infrastructure unique. Dès 1998, la standardisation du modèle de visioconférence sur IP (H323) préfigurait tout le potentiel de la téléphonie sur IP, mais aussi tous les problèmes issus de cette convergence des infrastructures voix, données et vidéo.

Les principales étapes de la ToIP



Une histoire de technologie et de coût

Outre les fournisseurs de technologies et quelques « primo adopteurs », d'autres facteurs ont largement contribué à l'arrivée et au développement des technologies permettant la convergence, comme notamment la dérégulation du marché des télécommunications. Celle-ci, initiée aux Etats Unis dans les années 1980, puis en Europe et enfin en France dans les années 1990, a rapidement favorisé l'apparition d'offres innovantes, principalement sur le marché résidentiel, avec l'Internet haut débit et la téléphonie sur IP, à des coûts extrêmement compétitifs... allant parfois jusqu'à la gratuité quasi-totale des consommations comme pour la téléphonie résidentiel fixe. La dérégulation du marché a également orienté les entreprises vers les technologies IP pour leurs communications téléphoniques, avec l'objectif de réaliser des gains financiers aussi importants que ceux réalisés par les particuliers.

Une histoire d'adaptation de l'organisation

Paradoxalement, bien qu'éminemment technologique, la convergence de la téléphonie et des réseaux informatiques a dans un premier temps conduit beaucoup d'entreprises à une convergence organisationnelle. En effet, au début des années 2000, rares étaient les DSI à disposer au sein de leur organisation de la responsabilité de la gestion de la téléphonie. Il leur a donc fallu à la fois incorporer les experts de la téléphonie de l'entreprise et surtout, comme pour toutes nouvelles applications métier, appréhender le périmètre, les besoins et les contraintes du monde de la téléphonie d'entreprise, ainsi que ses interactions avec le système d'information (annuaire, messagerie, etc.).

Une histoire de révolution dans l'usage de la téléphonie

D'un point de vue purement fonctionnel, la convergence, qui a commencé dès la fin des années 1990 par le transport de la voix sur IP (VoIP), s'est lentement transformé en téléphonie sur IP (ToIP) en remplaçant progressivement les PABX traditionnels. Depuis 2006, elle s'est métamorphosé en communications unifiées, un concept beaucoup plus large, qui associe téléphonie, visiophonie, visioconférence, travail collaboratif, messagerie de l'écrit et vocal, gestion de présence, acheminement intelligent, mobilité. Qu'elle soit appelée convergence ou communication unifiée, cette nouvelle tendance a considérablement modifié l'usage des moyens de communication de l'entreprise en les plaçant encore plus au cœur des relations entre collaborateurs mais également, au cœur des relations avec les partenaires et les clients.

Une histoire d'infrastructure

La simple transposition du service téléphonique sur une infrastructure de communication unique a eu d'importants impacts sur l'évolution de cette infrastructure. Elle a dû évoluer pour fournir les meilleurs niveaux de performance, de disponibilité et de sécurité exigée par la téléphonie. Au delà des batailles industrielles portant sur le choix de(s) protocole(s) pour la téléphonie sur IP, le transport de flux téléphoniques, dont le temps réel reste la principale contrainte, a considérablement modifié la manière même de concevoir ces infrastructures, qu'il s'agisse du WAN ou des infrastructures LAN. Ces contraintes ont rapidement conduit les fournisseurs de solutions d'infrastructure et les concepteurs d'architecture à reconsidérer certains aspects quelque peu négligés auparavant : la qualité de service (il fallait être en mesure de restituer une qualité de communication au moins aussi bonne que les solutions traditionnelles) et la sécurité, aussi bien en termes de confidentialité que de disponibilité et de stabilité.

La maîtrise de la qualité vocale

Comment restituer la qualité des communications voix dans une infrastructure IP ?

Un défi difficile à relever

La perspective de transporter des paquets IP contenant un flux téléphonique sur une infrastructure de communication IP a dans un premier temps été prise comme un sérieux défi à relever par les responsables des infrastructures. Les contraintes temps réel de la voix et le fonctionnement intrinsèque des infrastructures IP semblaient en effet inconciliables. Afin de répondre rapidement au besoin de gestion de la qualité de service sur les infrastructures IP, l'« IETF » (Internet Engineering Task Force) qui préside à l'évolution des standards Internet, engagea successivement plusieurs groupes de travail sur la manière de gérer la qualité de service IP.

De l'approche « Integrated Services » à l'approche « Differentiated Services »

Après un premier travail sur une approche dite « IntServ » (Integrated Services) qui s'avèrera rapidement peu efficace en pratique et surtout difficilement exploitable à grande échelle, l'« IETF » travailla à une approche bien plus adaptée au mode de fonctionnement du protocole IP nommé le modèle « DiffServ » (Differentiated Services). Le modèle « DiffServ » consiste à différencier le trafic par classes et à traiter chaque classe de service de proche en proche en se basant sur le marquage d'un champ « DSCP » (DiffServ Code Point) dans l'en-tête de paquet.



Le modèle de « DiffServ » est celui qui a été généralisé pour la gestion de qualité de services dans l'environnement IP. Il présente également l'avantage d'être applicable, aussi bien à la version actuelle du protocole IP (IPv4) qu'à sa version 6 (IPv6), sensé remplacer la version 4 à terme.

De plus, le type de marquage et les grands principes de priorisation mis en œuvre dans le modèle « DiffServ » pour les protocoles IP, sont directement compatibles avec ceux mis en œuvre par les autres protocoles généralement utilisés conjointement à IP, tel que MPLS, Ethernet, 802.1p, etc.

Correspondance du marquage		
DSCP	X X X Y Y 0	IPv4 IPv6
Précédence	X X X	IPv4
COS	X X X	MPLS
COS	X X X	802.1p
<small>XXX => Classe de service YY => Pondération perte de paquet</small>		

**La classification
des flux a permis
de déployer
l'approche
« Differentiated
Services »**

La prise en compte de la gestion de la qualité de service selon le modèle « DiffServ », implique l'identification des flux et leurs classifications. De vastes chantiers de recensement ont conduit à l'identification et la classification des flux de l'entreprise bien au-delà de la simple problématique de la qualité de la voix. Ce recensement a ainsi permis une meilleure connaissance des flux transitant sur l'infrastructure de communication de l'entreprise et a bien souvent permis d'identifier les flux licites et de contrôler voire interdire certains flux illicites. Il s'en est souvent suivi une prise de conscience des risques potentiels encourus au travers des infrastructures de communication IP et dans de nombreux cas cela a permis le déclenchement de démarches de sécurisation de l'infrastructure de communication. La mise en place de la qualité de service « DiffServ » a dans un premier temps été réalisée pour les infrastructures Wan. Ainsi, les offres de services des opérateurs en télécommunication ont rapidement permis de différencier le traitement des flux selon le modèle « DiffServ ».

Les infrastructures Wan sont effectivement celles qui nécessitent le plus d'attention puisque la bande passante est faible et la latence importante. Mais assez rapidement, le recensement et l'identification des flux ont été menés plus en profondeur sur les Lans et dans les centres informatiques bien souvent pour des raisons de sécurité plus que de qualité de service. La restitution de qualité des flux voix est aujourd'hui technologiquement maîtrisée. L'industrie s'oriente désormais vers des solutions permettant d'aller au-delà de la qualité des réseaux numériques comme RNIS en doublant littéralement le spectre de fréquence de 3 KHz à 7 KHz de bande passante.

Le challenge de la disponibilité

Comment garantir une disponibilité du service de téléphonie sur IP du même niveau que les solutions traditionnelles ?

Le challenge de la disponibilité d'une infrastructure IP

Hormis la capacité de l'infrastructure de communication à restituer la qualité des communications voix, voire même l'améliorer, les infrastructures de communications doivent en plus être en mesure de maintenir un niveau de disponibilité équivalent à celui des solutions téléphoniques dites traditionnelles. Il est vrai que la fiabilité des solutions traditionnelles « PABX » n'a cessé de s'améliorer au cours de leurs 20 à 30 années d'existence, ce qui leur permet aujourd'hui d'afficher un indicateur de disponibilité dont la valeur communément admise est de 99,999 %, soit une indisponibilité de moins de 5mn30 par an...

Le ressenti par les utilisateurs de la disponibilité des infrastructures de communications IP est probablement assez loin des cinq « 9 », même si les infrastructures de communication ne sont pas nécessairement la cause des indisponibilités subies par l'utilisateur. De fait, tout déploiement d'un service de téléphonie sur IP doit souvent être précédé d'une refonte ou au moins d'une adaptation des infrastructures de communications de l'entreprise visant notamment à augmenter le niveau de disponibilité.

Assurer un niveau de disponibilité équivalent à celui des installations téléphoniques classiques sur une infrastructure de communication répartie comme l'est celle d'un réseau d'entreprise recouvre différents aspects.

L'émergence d'infrastructures physiques maillées

Dans un premier temps, l'infrastructure physique (principalement le câblage entre les locaux techniques) doit disposer de cheminements différenciés pour les liaisons optiques afin d'offrir le maximum de chemins redondants. Contrairement aux infrastructures exclusivement dédiées aux transports de données (où l'ensemble des flux convergent du local technique d'accès vers le cœur de réseau puis vers le centre informatique, l'accès Wan ou l'Internet), la téléphonie modifie considérablement la matrice habituelle des flux. Le flux généré par une communication téléphonique sur IP s'établit directement entre les postes IP des utilisateurs. Lorsque ceux-ci sont situés au même étage d'un immeuble mais accèdent physiquement à l'infrastructure sur deux locaux techniques différents, le flux téléphonique est acheminé d'un local technique d'accès vers le cœur de l'infrastructure, pour remonter au même étage vers l'autre local technique d'accès et inversement. Afin d'éviter de surcharger inutilement les équipements du cœur de réseau et leurs liaisons, il est préférable d'établir des liaisons directes entre les deux locaux techniques. Cette solution peut également être appliquée aux locaux techniques d'étages adjacents d'une même colonne montante.

En résumé, la matrice des flux traditionnellement observée et relativement déterministe, est aujourd'hui rendue beaucoup plus aléatoire avec l'arrivée des flux téléphoniques, ce qui favorise l'émergence d'infrastructures physiques beaucoup plus maillées, donc plus résilientes et donc plus disponibles.

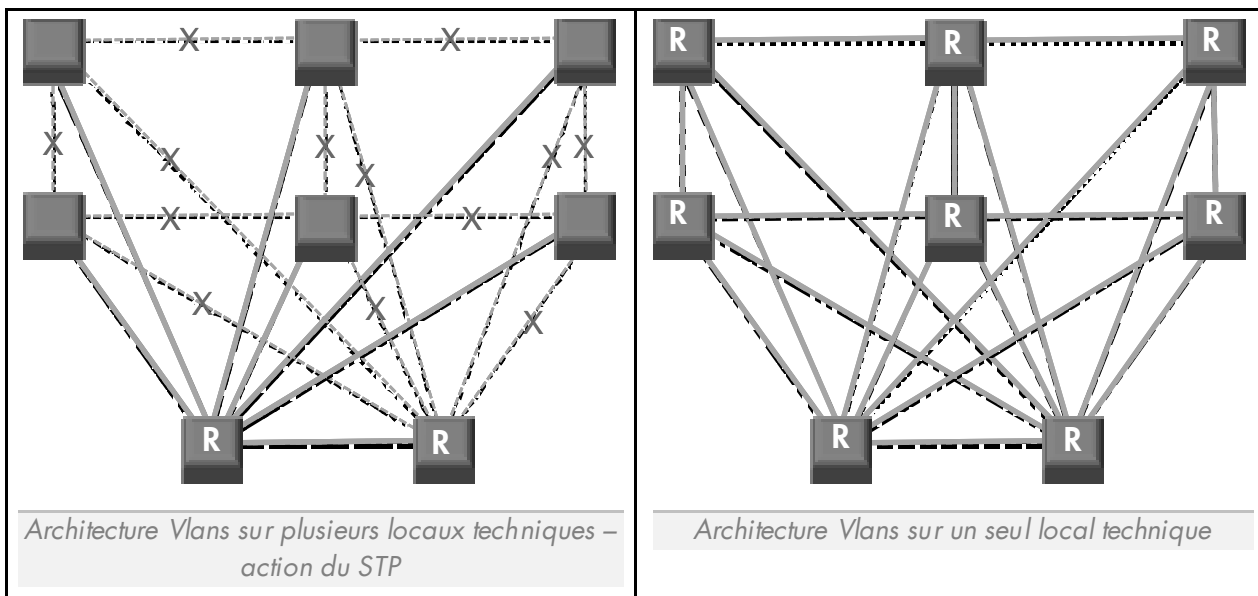
De plus, si la bande passante unitaire d'une communication téléphonique n'est pas très importante (environ 80 Kbps aujourd'hui), les futurs codecs haute qualité consommeront de l'ordre de 200 Kbps. A terme, la démocratisation de la visioconférence et de la visiotéléphonie atteindront pratiquement 1 Mbps par sens de communication (et plus encore avec la visioconférence haute définition) et toujours avec de très fortes contraintes temps réels.

L'adaptation de l'architecture logique au maillage de l'infrastructure physique

Dans un second temps, c'est au niveau de l'architecture logique que va se focaliser le travail le plus important. Le recul dont on dispose en terme d'infrastructures IP (particulièrement en ce qui concerne le LAN) permet d'orienter rapidement les nouvelles architectures vers des règles de design simples, efficaces et permettant d'assurer notamment un meilleur niveau de disponibilité. L'un des principaux facteurs d'instabilité d'une infrastructure de type Lan provient généralement de la combinaison d'une topologie physique redondante et de la propagation des mêmes Vlans sur plusieurs locaux techniques. Ceci engendre des boucles au niveau 2 (modèle OSI) qui dans le cas d'Ethernet paralyse le réseau. Le protocole STP (Spanning Tree Protocol) permet de redéfinir une topologie logique sans boucle (en bloquant certains liens) avec des chemins de secours en cas de panne, mais il s'avère peu stable et lent à converger en cas de problème. Plusieurs versions successives du protocole STP n'ont pas permis de garantir la stabilité et la convergence rapide des infrastructures quand le niveau 2 est propagé entre plusieurs locaux techniques. De plus, le protocole STP procède par blocage de liens afin d'éviter les boucles, donc il impose de ne pas utiliser certains liens, ce qui sur une infrastructure physique vouée hautement disponible et donc fortement maillée devient contreproductif.

En attendant un protocole permettant la construction d'infrastructures de niveau 2 supportant des chemins multiples et donc les boucles, il faut donc :

- soit supprimer les liens redondants pour éviter l'usage du protocole STP
- soit éviter de propager les Vlans sur plusieurs locaux techniques.



Pallier les limites du protocole STP

C'est évidemment la limitation des Vlan à un seul local technique qu'il faut choisir. Pour cela, il faut revoir certains concepts d'architecture comme par exemple limiter la portée d'un Vlan à un seul local technique et utiliser des fonctions de routage entre chaque local technique. Ce type d'architecture routée permet :

- une utilisation optimale des infrastructures physiques surtout lorsqu'elles sont maillées ;
- un allègement des équipements de cœur de réseau en limitant au strict nécessaire le flux qui les traverse ;
- une stabilité élevée ;
- l'amélioration de la vitesse de convergence du réseau grâce à des protocoles largement éprouvés comme OSPF ;
- une meilleure maîtrise des incidents : investigations facilitée en cas d'incident, limitation des impacts, réduction à un local technique de la portée de certaines attaques ;
- de manière générale, meilleure gestion de l'infrastructure de communication.

La mise en place de ce type d'architecture dite « routée » nécessite une réflexion préalable au niveau du plan d'adressage IP. Elle impose un certain nombre de modifications des équipements de l'infrastructure et la modification des serveurs DHCP. Ces opérations sont souvent rendues nécessaires par ailleurs, pour prendre en compte la téléphonie sur IP et les projets de mobilité Wifi, de contrôles d'accès à l'infrastructure et de solutions de contrôle de conformité des stations de travail.

La confidentialité des échanges

Comment s'assurer de la sécurité du service de téléphonie sur IP ?

La confidentialité des échanges est un point clef de la ToIP

En termes de sécurité ou plus précisément de confidentialité, le risque d'écoute des communications par un tiers, accédant ou disposant de moyens d'accès aux infrastructures de communications de l'entreprise, a rapidement été identifié comme un risque majeur par les entreprises. Ces aspects ont été pris en compte de trois manières différentes et complémentaires comme c'est souvent le cas en sécurité (multiplier les lignes de défense, pour accroître le niveau de sûreté).

La première mesure est comme souvent, d'ordre organisationnelle et conduit à la mise en place de dispositifs et de procédures permettant de maîtriser l'accès physique aux locaux.

La seconde mesure a été la mise à disposition par les fournisseurs de fonctionnalités sur les équipements d'infrastructure qui permettent de limiter les attaques aboutissant à une recopie du flux téléphonique à des fins d'écoute illégale.

La troisième mesure est aujourd'hui proposée par la plupart des grands acteurs du monde de la téléphonie d'entreprise. Elle consiste à chiffrer les communications IP et, pour certaines offres, à chiffrer également les flux de signalisation qui assurent l'établissement des communications téléphoniques.

La ToIP plonge la Téléphonie au cœur des menaces sur l'infrastructure IP

En termes de sécurité proprement dite, la convergence de la voix et des données a favorisé l'apparition de solutions de sécurité de plus en plus intégrées à l'infrastructure. Elles permettent de s'attaquer aux attaques ou intrusions qui proviennent de l'intérieur même de l'infrastructure. Aujourd'hui les moyens de défense des infrastructures sont principalement périphériques et protègent essentiellement de l'extérieur (principalement de l'Internet), alors que l'on sait depuis longtemps que ce modèle est mal adapté aux menaces dites « internes » qui sont estimées à 70% des attaques ou des actes malveillants, volontaires ou non.

Dans le cadre de la mise en place d'un service de téléphonie, il est donc nécessaire de se prémunir de ce genre d'attaques. Là encore, des approches différentes mais complémentaires sont mises en œuvre pour accroître le niveau de sécurisation de l'infrastructure de communication vis-à-vis d'actes provenant de l'intérieur de l'entreprise.

Tout d'abord, l'approfondissement des concepts classiques de « défense en profondeur », multipliant les barrières de protection ont aujourd'hui leurs places au cœur des infrastructures de communications. Et ceci grâce aux évolutions technologiques (performance des équipements, virtualisation). Il est en effet concevable aujourd'hui de protéger l'infrastructure en positionnant des barrières de protection de type pare-feux, détecteurs d'intrusions, SBC à très haut débit, directement au cœur même des infrastructures et notamment au sein du centre informatique.

Un autre moyen de sécuriser l'infrastructure de communication d'actes malveillants ou d'attaques internes consiste à n'autoriser l'accès au système d'information de l'entreprise qu'au personnel dûment authentifié. Les autres utilisateurs sont alors soit cantonnés à un environnement restreint (par exemple l'accès Internet public), soit, purement et simplement, interdits d'accès à l'infrastructure.

En outre, il peut être intéressant de s'assurer que l'utilisateur se connecte avec une station de travail conforme aux recommandations de la politique de sécurité de l'entreprise. En fonction de l'état de conformité de la station, il est possible de graduer plus ou moins l'ouverture du système d'informations.

Ces deux approches sont applicables dans le cadre de la sécurisation de l'infrastructure de communication filaire de l'entreprise mais sont parfaitement transposables dans les solutions de mobilité, quelles soient internes à l'entreprise comme le Wifi ou bien externes à celle-ci : hot spot, web café, accès clients, accès partenaires ou bien encore, le télétravail de collaborateur.

Le contrôle d'accès de l'utilisateur

Cette première approche a pour objectif d'assurer l'authentification de l'utilisateur avant même de lui donner accès à l'infrastructure de communication l'entreprise. L'authentification peut-être réalisée de manière plus ou moins forte, en fonction de l'adresse de la station, du nom d'utilisateur et de son mot de passe, d'un certificat chiffré, d'un dispositif de lecteur biométrique, etc. Ce contrôle d'accès est réalisé au travers du protocole standard 802.1X. Il a initialement été défini pour assurer l'authentification d'accès des utilisateurs au réseau sans fil Wifi. Il a ensuite été généralisé pour le contrôle d'accès aux infrastructures filaires pour lequel il nécessite un petit logiciel (supplément) coté station de travail et un commutateur supportant ce standard 802.1X.

La mise en œuvre d'une solution de contrôle d'accès basée sur ce protocole permet, en cas d'échec à l'authentification, d'interdire purement et simplement l'accès de l'utilisateur à l'infrastructure ou bien son confinement dans un sous-réseau Vlan disposant de droits limités. En revanche, en cas d'authentification réussie, l'utilisateur a non seulement accès à l'infrastructure de communication mais peut automatiquement être positionné dans son Vlan en fonction du groupe auquel il appartient (comptabilité, commercial, etc.) et donc, son propre environnement de travail avec les droits liés à son groupe.

La base d'authentification des utilisateurs est centralisée sur un serveur radius capable si nécessaire, d'interroger l'annuaire de l'entreprise ou une autorité de certification. Le contrôle d'accès de l'utilisateur permet donc d'accroître le niveau de sécurité de l'infrastructure de communication en isolant ou bien en écartant les utilisateurs non authentifiés potentiellement dangereux. Le même protocole 802.1X permet dans le cadre de solution de la téléphonie sur IP d'assurer l'authentification des postes téléphoniques IP avant de les accueillir sur l'infrastructure.

Le contrôle de conformité du poste de travail

Le contrôle de conformité du poste de travail a pour objectif d'écartier le poste de travail qui ne respecte pas les règles de sécurité édictées par la politique de sécurité de l'entreprise . Les postes travail clairement identifiés comme ne faisant pas partie du parc informatique de l'entreprise peuvent alors être positionnés dans un vlan de quarantaine ou purement interdits d'accès à l'infrastructure ou encore accueillis dans un vlan limitant drastiquement l'accès au système d'information.

Pour les postes de travail clairement identifiés comme étant des postes de l'entreprise, deux cas de figure sont possibles :

- le poste de travail est conforme ; auquel cas il accède à l'infrastructure et à son propre environnement
- le poste de travail n'est pas parfaitement à jour et il est orienté vers un Vlan qui lui donne accès à un système de médiation qui a en charge la mise en conformité du poste avant un nouveau contrôle.

Le caractère sensible de la téléphonie pour bon nombre d'entreprises a incité les principaux fournisseurs de solutions et les organismes de standardisation ou de normalisation à étudier puis proposer à celles-ci de nombreuses fonctionnalités permettant d'accroître de plus en plus la disponibilité et la sécurité des infrastructures de communication.

Ces évolutions sont devenues tellement importantes qu'aujourd'hui on ne conçoit plus une infrastructure sans prendre en compte, dès les phases initiales de définition, sa sécurisation et la manière de la gérer. Il n'est plus rare de voir des architectures logiques de centre informatique totalement articulées autour des fonctions de sécurité comme les pare-feux et autres détecteurs d'intrusions, ni de voir des projets de fédération d'annuaires gérant à la fois les droits d'accès à l'infrastructure, aux ressources et aux applications.

